PracticeOne
Application Service Provider Privacy & Security Policies

Access	o Physical Access is restricted via bio metrics to facility and locked cabinets to h/w. o Employees have access to the customer's data. o Customers only have access to customers data 1. Oracle Database row security 2. Proprietary PM Client. Login info required 3. Login info required to HTTPS EHR site. o All clients accessing the product are required to use Microsoft's Internet Explorer version 6.0 or above with TLS 1.0 (check TLS 1.0 in Tools – Internet Options – Advanced). If TLS is not checked, the client will not be able to access the product. o Firewall. Only specific ports granted for in & outbound traffic. o Web server is required to enable local security policy setting "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing".
Authorization	o Physical Access Granted by collocation authority. o Each client must execute a HIPAA Business Associate Agreement with PracticeOne
Authentication	o Electronic Health Record 1. IIS servers are setup to require SSL/TLS by checking "Require secure channel (SSL)" under Directory Security setup in IIS management (for both web services and product directories) and set their local security policy to "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing". Requiring SSL and setting the local policy to require FIPS compliant algorithms ensures that client requests must be TLS 1.0 enforcing TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher technology. 2. The default mode of TLS authentication with cipher suite TLS_RSA_WITH_3DES_EDE_CBC_SHA is server-only or mutual authentication using certificates. The Querying node acts as a TLS client, and the Responding node acts as a TLS server. 3. To authenticate the Web server, the client Web browser checks the certificate store (Trusted Root Certification Authorities). All certificates are obtained from trusted CAs, allowing certificates to be stored on the client. On each session request to login (and access PHI data) client Web browsers create a unique session key. The browser encrypts the session key with the certificate so that only the web server with matching key can decrypt (and resend data back encrypted) ensuring the authenticity of the remote node request and response. o Practice Management System 1. The e-Medsys PM Application Server can run with SSL either enabled or disabled. It is also possible to have more than one instance of the Application Server software running on a single Application Server. We call this having multiple "runservers". SSL can be enabled on one run server and disabled on another. This is a useful scenario in some environments. PracticeOne has incorporated several security measures into the design of the e-Medsys client software with respect to data traffic between it and the remote Application Server. 2. First, to increase throughput between the client and application server, e-Medsys compresses most of the data traffic. As a byproduct, this suppresses most clear text sent across the network or over the Internet

	even if SSL is not enabled on the runserver. 3. Second, we have embedded an SSL certificate within the e-Medsys client software and the Application Server software. 4. Third, in our implementation of SSL, we use a Java package called Java Secure Socket Extension or JSSE which supports the 3DES Cipher Suite.
Audit	o P1 audit tables o Oracle audit tables o Firewall logs
Secondary Uses of Data	o Permitted uses under the Business Associated Agreement: 1. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION 1.1. Software and Services. (a) Business Associate provides software and services (which may include billing, analytic and transaction services as well as servicing software products) ("Services") that involve the use and/or disclosure of Protected Health Information. These Services are provided to Customer under various agreements ("License Agreements") that specify the Services to be provided by Business Associate. Except as otherwise specified herein, the Business Associate may make any and all uses and disclosures of Protected Health Information created or received from or on behalf of Customer necessary to perform its obligations under the Service Agreements. (b) Business Associate may perform Data Aggregation for the Health Care Operations of Customer. 1.2. Public Health Activities. Business Associate may use, analyze, and disclose the Protected Health Information in its possession for the public health activities and purposes set forth at 45 C.F.R. § 164.512(b) 1.3. Business Activities of the Business Associate. Unless otherwise limited herein, the Business Associate may: (a) consistent with 45 C.F.R. § 64.504(e)(4), use and disclose the Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate; and (b) de-identify any and all Protected Health Information in accordance with 45 C.F.R. § 164.514(b). Customer acknowledges and agrees that de-identified information is not Protected Health Information and that Business Associate may use such de-identified information for any lawful purpose.
Data Ownership & Transfer	o Customer owns data o But charges apply for the extraction and delivery of data in CSV files or Oracle Data extraction formats. Cost from $2,000 to $3,000 depending on data and format to be delivered.
Disaster Recovery	o The PracticeOne Co-Location facility utilizes redundant uninterruptable power supplies (UPS) and the facility has a diesel power generator if the area power grid should fail. o Data is backed-up daily to two mediums: 1. Servers with redundant disk storage 2. Cartridge tape back-up system – cartridge systems are rotated daily so a weeks worth of back-ups are always available o One set of weekly back-ups are stored offsite in a second location to ensure recovery in case of fire, water or other type of damage to the collocation facility. o PracticeOne's ASP utilizes Raid 5 drive configurations for the most robust protection against drive failure. o Oracle databases are in archive log mode. This allows for the possibility to recover up to the minute of failure."